5 FAH-4 H-200
RECORDS ORGANIZATION

5 FAH-4 H-210
DEPARTMENT OFFICES, FIELD OFFICES, AND POSTS

(TL:RMH-3; 06-15-2000)

5 FAH-4 H-211 GENERAL

(TL:RMH-3; 06-15-2000)

a. Records are created to document the organization, functions, policies, decisions, procedures, operations, or other activities of the Department and posts. To ensure the preservation of records, each bureau, office and post must organize and maintain documents that it produces or receives in accordance with the standards and procedures contained in this Handbook and appropriate Foreign Affairs Manuals and Handbooks relating to information and security management and policy and procedures.

b. Unless otherwise specified, these procedures apply to all Department of State domestic offices, including field offices and all Foreign Service posts, missions, special interest sections, international organizations, and other operations such as the *Financial Service Centers (FSC)*. Other agencies at posts abroad must follow their own records management procedures.

5 FAH-4 H-212 RECORDS CREATION—GENERAL METHODS AND PROCEDURES

(TL:RMH-1; 10-30-1995)

The following methods and procedures for the creation of records are to be followed by all offices and posts on a continuing basis:

(1) Survey of Office/Post Procedures—All existing and proposed office/post procedures are to be subject to continuing examination for their effect on recordkeeping. Wherever possible, such procedures are to be revised, consolidated, or eliminated to prevent the creation of unnecessary records.

(2) Elimination of Duplicate Files—Every bureau, office, and post will take positive action to prevent the establishment of, or to eliminate, duplicate files not required for current operating purposes. Proliferation of individual office working files can be controlled through careful planning at the division or branch level and by maximum use of the Department's Central Foreign Policy File.

(3) Limitation on the Number of Copies—The number of copies of communications and other documents reproduced and distributed is to be limited to those required on a strict need-to-know basis. To the extent feasible, control is to be exercised to prevent the reproduction of unnecessary copies. As a general rule, information copies are not to be filed with official records but rather maintained in a chronological, post, or other temporary file which is retained for only a short period of time.

5 FAH-4 H-213 SEPARATION BY SECURITY CLASSIFICATION, CHANNEL AND CAPTION

(TL:RMH-1; 10-30-1995)

Offices and posts must follow pertinent security procedures in 12 FAM and associated security handbooks to determine how best to file and adequately protect classified and unclassified but sensitive material.

5 FAH-4 H-213.1 General

(TL:RMH-1; 06-15-2000)

The following procedures apply to Department offices and posts (see 5 FAH-4 H-213.2 for additional procedures applicable to Department offices and 5 FAH-4 H-213.3 for those applicable to posts):

(1) Documents bearing the special distribution captions NO DISTRIBUTION (NODIS) or EXCLUSIVE DISTRIBUTION (EXDIS) *shall be treated as NOFORN. These* documents must be given the physical protection prescribed *by their classification. See 12 FAM 539 for additional guidance.*

(2) Documents bearing the captions LIMITED DISTRIBUTION (LIMDIS) and STATE DISTRIBUTION ONLY (STADIS), and bearing no other captions, may be filed with unrestricted material of the same security classification, but with access limited to need to know. LIMDIS documents must be given the physical protection required by their classification. STADIS materials, which may also be captioned EXDIS or LIMDIS must be given physical security appropriate to their *classification*.

(3) All NODIS and EXDIS documents (i.e. telegrams, memoranda and letters) are automatically decaptioned after five years unless exempted by S/S. The storage of decaptioned but still classified documents should afford a level of protection appropriate to their classification.

5 FAH-4 H-213.2 Department Offices

(TL:RMH-1; 10-30-1995)

a. Action documents and telegrams captioned NODIS and EXDIS are maintained by the Executive Secretariat only. When captioned material is no longer needed, the bureaus should destroy their copy(ies).

b. Special channel messages are distributed from the communications center only to the action bureau. Bureaus having their own channel is to establish procedures and guidelines for the security of these messages, how these messages are filed, maintained, and who has access to them. While not all messages will be classified, most contain sensitive information.

5 FAH-4 H-213.3 Posts

(TL:RMH-1; 10-30-1995)

a. For critical and high threat posts, the segregation of classified and unclassified materials is required to allow for rapid destruction of classified materials.

b. All other posts can separate or commingle classified and unclassified records based upon the ease of destruction in an emergency. Over and above the availability and capability of destruction equipment, probably the most significant factor in separating classified from unclassified is the physical volume of classified records involved.

c. The following procedures are to be used to process **TOP SECRET** traffic on the **TERP V** systems (TOP SECRET material can only be maintained in paper form. These messages will not be stored on any hard drives, floppies or other media once it has been received and processed) :

(1) Upon receipt of TOP SECRET traffic, the operator makes sure it is processed and a hard copy is printed,

(2) Once the telegram has been printed and stored, the operator retrieves the message and enter the “EDIT” mode. (Note: The time required for a telegram to be stored will vary on how active the TERP V system is at the time.)

(3) After entering the edit mode, use the “F6” (Line Delete) key to delete the text of the message, leaving only the header and end of message (EOM) functions. (Note: If the telegram is more than one section, each section will have to be retrieved and the text deleted.)

(4) Once all of the text has been deleted, save the remainder of the message using the “FLO” (Save Changes) key. The TERP V system will save the file in the same area on the SCSI drive as it was originally stored, and,

(5) Exit the Retrieve function and continue with normal processing.

d. Documents bearing the special distribution captions NO DISTRIBUTION (NODIS) or EXCLUSIVE DISTRIBUTION (EXDIS) are maintained in the Information Program Center (IPC) and kept separate from other documents.

e. Unclassified, and Limited Official Use (LOU), now known as Sensitive but Unclassified (SBU), records may be maintained together, if all persons having access to those files have been authorized, i.e., have an established need to know, and if security conditions at post warrant such access.

f. NARPLUS and NAROP captioned documents are kept by the action office and afforded physical protection appropriate to their security classification.

g. Action copies of AGREMENT, DIRGEN, DISSENT, FI and ROGER channel messages are not kept in the action office, but in the IPC. Sections may file dummy copies in their chronological files for continuity sake.

h. Grievance channel messages are kept by the action addressee only, with a dummy copy maintained in the IPC.

i. MED and DS channel messages are maintained by the action office, with a dummy copy included in the IPC.

j. All other channel captioned messages are kept in the action office, with a copy included in the IPC.

k. Certain categories of unclassified files may contain sensitive information, and are stored and handled as if they were classified.

l. The responsible official at post applies the Terminal Equipment Replacement Program (TERP) “store inhibit” function to those authorized channel caption telegrams that require a dummy copy in the IPC post chronological file and storage of the action copy in the Post Communications Center (PCC). These telegrams are deleted or archived off Classified Information Handling System (CIHS) media once processing is completed.

5 FAH-4 H-213.3-1 Continuous Actions

(TL:RMH-1; 10-30-1995)

a. The Information Management or Information Program Officer sees that the following actions are taken on a regular basis for the security of information at posts.

(1) Keep classified, substantive files to a minimum through periodic review.

(2) Accelerate retirement of front office, political and economic program files.

(3) Distribute information copies as “read and destroy” and limit distribution to those who “need-to-know.”

(4) Identify and mark sensitive but unclassified documents and include in the post destruction planning.

b. Examples of sensitive but unclassified documents include (See 12 FAM for definition of sensitive but unclassified):

(1) Blank passports;

(2) Consular stamps and seals;

(3) Biographic or investigative files (including those of other agencies such as DEA, INS, Customs, Legatt, etc.);

(4) Security investigative files and indices;

(5) Visa and passport/citizenship fraud files;

(6) Visa refusal files (categories I and II);

(7) Immigrant visa control cards (FS-499) (OF-224B), and immigrant visa petitions with supporting material in visa A-Z files;

(8) Personnel folders, including those of foreign national employees;

(9) Leave records;

(10) Employee medical records;

(11) Business, commercial, and USIS contact(s) files; and

(12) Budget and fiscal (B&F) records, such as representational vouchers, lists of contract employees, and other files showing contacts.

5 FAH-4 H-213.3-2 Planning

(TL:RMH-1; 10-30-1995)

Prior to the establishment, or as a periodic review procedure, of an official file system, the post's security officer and the post's information management or information program officer, accomplishes the following:

(1) Verifies that the present physical and procedural security is satisfactory as it applies to existing file systems;

(2) In areas of political instability, review emergency destruction procedures and equipment to see that all requirements are being met; and,

(3) Brief offices on security of files and sees that the files destruction procedures are covered in the emergency evacuation procedures.

5 FAH-4 H-214 OFFICIAL FILE SYSTEM

(TL:RMH-1; 10-30-1995)

a. The official file system for the Department of State is the TAGS/Terms System. TAGS is an acronym for Traffic Analyses by Geography and Subject. See 5 FAH-3 for guidance on the use of this system for both paper and electronic records. See 5 FAH-4 H-219 of this handbook for procedures on non-paper records.

b. Large series of case files (e.g., personnel, investigative, voucher, contract etc.), chronological files and files of printed and processed publications that are not appropriate for arrangement by subject need not be arranged by the TAGS/Terms System.

c. The Office of Inspector General (OIG) files are exempt from this requirement and are maintained in accordance with the Privacy Act notice published in the Federal Register (56 FR 7071, February 21, 1991). For more information regarding OIG files, see 2 FAM.

5 FAH-4 H-215 BLOCKING

(TL:RMH-3; 06-15-2000)

All official files will be maintained in one-year blocks. Exceptions to this requirement, based on small volume or other considerations, require the approval of the *Office of IRM Programs and Services (A/RPS/IPS)*. Files must be blocked on a calendar year basis, except where a fiscal year basis is more appropriate. This promotes efficiency in filing, retrieval, and disposition. Case files may be kept in an "active" or "inactive" file; or may be incorporated into basic program files, as appropriate, using the correct TAGS. Inactive files are to indicate a cut-off period, such as by year or a specific date. See 5 FAH-4 H-219 for procedures on non-paper records.

5 FAH-4 H-216 TYPES OF DOCUMENTARY MATERIALS

(TL:RMH-1; 10-30-1995)

Documentary materials of the Department consist of six categories:

(1) central files,

(2) chronological files,

(3) program files,

(4) reference materials,

(5) working files, and

(6) personal papers.

5 FAH-4 H-216.1 Central Files

5 FAH-4 H-216.1-1 Department Offices

(TL:RMH-3; 06-15-2000)

a. **Content**. There are several major central files in the Department:

(1) *SAS (State Archiving System)*, which is the central foreign policy file;

(2) Personnel Records;

(3) Financial Records; and

(4) Other operational records, such as Passport records.

These files reflect the official documentation of an organization's activities in specific areas or missions, as identified in 5 FAH-4 H-211 above. These files can be automated or paper. The offices responsible for these files, such as PER and *A/RPS/IPS*, establish the guidelines and procedures for maintenance, retirement, transfer, and retrieval. For specific guidance on these files, contact the responsible offices.

b. **Decision to Centralize**. The decision to centralize files depends on the type of information and the needs of the bureau or organization to effectively meet its mission. Factors to be considered in deciding whether or not to centralize include:

(1) Size and location of the organizational elements within a bureau;

(2) Degree of physical protection needed;

(3) Adequacy of space and filing facilities;

(4) Adequacy of human resources to manage the files; and,

(5) Training and experience in maintaining files.

c. **File Management**. Each program, bureau, or office that maintains a major central file must assign a responsible person to manage the operations of the file, ensure the integrity of the data, and assist in access to, filing, and disposition of data. The responsible person must have received training in the basic practices and principles of records management and maintain active contact with *A/RPS/IPS*.

d. **File Arrangement**. All records in a specific category that have been authorized for maintenance in a central file must be filed so that the record of events is complete and accurate. Division of records between a central file and an operating unit's subject/program or working files can lead to duplication and lack of central integrity of information, as well as inhibiting effective retrieval. Offices must see that procedures exist that explain to all personnel the operations of the central file.

5 FAH-4 H-216.1-2 Posts

(TL:RMH-3; 06-15-2000)

a. The establishment of central files at post is the exception to the rule, e.g., a very small post which houses all records in the IPC.

b. If a post decides to maintain its records in a centralized area, it must include all records that cover the issues mentioned in 5 FAH-4 H-210 above. Refer to 5 FAH-4 H-216.3-2 for procedures when files are not centralized.

c. File Management

(1) The officer in charge of the post's IPC is designated as the post records officer. The officer must have experience and training in management of records. This person is responsible for:

(2) Maintaining the central file, providing for the integrity of the data, assisting in access to, filing, and disposition of data. This person must maintain active contact with *A/RPS/IPS*, coordinate on-site training in records management, and provide technical assistance to post personnel.

(3) Coordinating the annual disposal of records and retirement of records to the Department's Records Service Center.

(4) Working with post security to provide adequate enforcement of security over records.

(5) Report in even-numbered years the status of records in the Biennial Records Report. See 5 FAH-4 H-312.3.

d. Completeness—All records in a specific category that are maintained in a central file must be filed so that the record of events is complete and accurate.

5 FAH-4 H-216.2 Chronological Files

(TL:RMH-1; 10-30-1995)

a. **Contents**. A chronological file consists of duplicate information copies of each incoming and outgoing communication, whether it be telegram, letter, report, etc. Chronological files are a valuable tool for quick retrieval of current information. Chronological files are not official files as prescribed in this chapter, and are only to be used as reference. The official file, which fully documents actions taken, will be found in the program files or central files. Exceptions to the rule are principal officer files. These files are permanent records to be retired.

b. **File Management**.

(1) Department Offices: Chronological files are usually maintained by a designated person, such as a secretary, who is responsible for their integrity, upkeep, security, and disposition. Chronological files may be kept in a centralized file or with office program files.

(2) Posts: Chronological files are usually maintained by a designated person, such as a secretary or information management officer, who is responsible for their integrity, upkeep, security, and disposition.

c. **File Arrangement**. By their nature, chronological files are usually maintained by date order. The file may also be arranged in separate incoming and outgoing series, alphabetically by post, or by serial number.

d. **Security.** Chronological files usually contain both unclassified and classified documents. Top Secret and special captioned documents are maintained separately (See 5 FAH-4 H-213).

5 FAH-4 H-216.3 Program Files

5 FAH-4 H-216.3-1 Department Offices

(TL:RMH-3; 06-15-2000)

a. **Content**. Program files consist of records relating directly to an organization or bureau's specific mission and are maintained in separate offices within an organization. They are the official documentation of that organization's activities, as identified in this section of the handbook. Information copies of documents that do not relate to the operations of an organization are to be destroyed while those that do relate are to be filed with appropriate program material. Program files also include drafts of documents that contain unique information, such as annotations or comments, that help explain the formulation or execution of agency policies, decisions, actions or responsibilities, and which were circulated or made available to employees other than the drafter for the purpose of approval, comment, action or to keep staff informed about agency business.

b. **File Management**. Each program, bureau, or office that maintains program files must assign a person to be responsible for managing the operations of the files, ensure the integrity of the data, assist in access, filing, and disposition of data. The responsible person must receive training in the basic practices and principles of records management and maintain a liaison with *A/RPS/IPS*.

c. **File Arrangement**. Program records are filed according to their general informational, or subject content. They can be arranged subjectively, chronologically, or by case.

5 FAH-4 H-216.3-2 Posts

(TL:RMH-3; 06-15-2000)

a. When a post decides not to centrally maintain all of its major files, then the following procedures apply:

(1) Program files consist of records relating directly to post mission and are maintained in each section of the post. They are the official documentation of post activities, as identified in this section of the handbook.

(2) Program files kept in sections usually consist of: administrative, consular, political, security, commercial, economic, personnel, and records of other agencies. Posts may decide to centrally locate only those records that are security sensitive.

b. **File Management**. Each section that maintains program files must assign a responsible person to manage the operations of the files, ensure the integrity of the data, assist in access to, filing, and disposition of data. The responsible person must have received training from the Post IPC in general records management policies and procedures (or A/RPS) and maintain active contact with them. The responsibilities are outlined in 5 FAH-4 H-216.1-2 c, File Management. The post information management or information program officer remains the primary single contact with the Department regarding records. Additionally, the responsible person must assist in periodic reporting of record holdings (see 5 FAH-4 H-312.3).

5 FAH-4 H-216.4 Reference Material

(TL:RMH-1; 10-30-1995)

Reference materials consist of magazines, books, and other types of publications, visuals, etc., that provide background information pertinent to an organization’s mission. They are not official documents. The materials are kept for as long as they provide information of value to an office, but are not to be retired with official files.

5 FAH-4 H-216.5 Working Files

(TL:RMH-1; 10-30-1995)

a. **General**. Working files are to be kept to an absolute minimum consistent with operating needs. The officer screens out official documents for incorporation in the appropriate program file and destroys the remainder of the file when projects or assignments are completed. If there are no centralized office files, the officer’s working files become the program files of the office. Some materials within working files might be appropriate for incorporation with reference materials, listed above.

b. **Content.** Working files usually consist of the following:

(1) Information or extra copies of communications and correspondence;

(2) Publications of the Department and other Federal agencies;

(3) Newspaper clippings;

(4) Rough drafts of documents and background data that do not record necessary approval or basic changes in text; and

(5) Reference materials.

c. **File Management**. Offices and posts may allow management of working files to be handled by individual employees. Offices, however, establish written policy regarding managing the working files belonging to retiring or resigning personnel or upon an employee's departure.

5 FAH-4 H-216.6 Personal Papers

(TL:RMH-1; 10-30-1995)

a. **Content**. Personal papers are documentary materials of a private or non-public nature that have not been used in the transaction of Department of State business. Personal papers include:

(1) **Papers Created or Received Before Entering Government Service**—These papers must not have been used subsequently in the transaction of Department business. Examples include work files from previous employment, political materials and reference files.

(2) **Private Papers Brought Into, Created or Received in the Office**—Examples include family and personal correspondence, documents relating solely to outside business interests or political and professional activities, manuscripts and drafts for articles and books, and volunteer and community service records. These papers must not be related to or used in the transaction of Department business. Correspondence received or sent as a Department official is not personal.

(3) **Personal Copies of Employment-Related Records**—Examples include personal copies of financial disclosure forms, travel vouchers or health insurance forms and literature.

(4) **Work-Related Personal Papers**—Examples include diaries, journals, notes and personal calendars and appointment schedules if they are for personal use only and not prepared for, used in, or communicated in the transaction of Department business. This is the most complex category of personal papers and often requires consultation with the Department Records Officer and the Office of the Legal Adviser. Whether these papers are personal or official depends upon an assessment of several factors including their creation, content, purpose, distribution, maintenance and use, disposition and control.

b. **File Management**. Personal papers must be filed separately from office records and clearly identified as personal. If information about both private matters and Department business appears in a document, the Department information is to be copied or extracted and incorporated into the official file. The personal correspondence may be considered as a personal paper if a full record of the official activities is preserved in the official file and if the information is unclassified.

5 FAH-4 H-217 NON-RECORD MATERIALS

(TL:RMH-1; 10-30-1995)

a. **Content**. Non-record materials are Department-owned documentary materials that do not meet the legal definition of a record. Non-record materials include:

(1) Convenience copies of agency records. Departing officials may request Department authorization to remove copies of unclassified agency records. Generally, these are copies of documents the official drafted, reviewed or otherwise acted upon, duplicated for the express purpose of maintaining a personal convenience or reference copy.

(2) Working Papers. Departing officials may request Department authorization to remove other unclassified non-record materials such as preliminary drafts not circulated for comment, working papers, and notes and similar items not suitable for preservation as a record by the Department. These types of documents may not be removed if they contain classified information.

b. **File Management.** Non-record materials are those that do not meet the legal definition of a federal record as described in 5 FAH-4 H-113. These documents are kept only for convenience or reference purposes and are to be destroyed when no longer needed.

5 FAH-4 H-218 REMOVAL OF PERSONAL PAPERS AND NON-RECORD MATERIAL

(TL:RMH-2; 4-15-97)

a. **Responsibilities.**

(1) The administrative section of each Department of State bureau, office, or post, is responsible for:

(a) Reminding all officials, about to leave the Department or a post, of the requirements for the removal of personal papers and nonrecord materials;

(b) Enforcing compliance with these procedures for the removal of documentary materials prior to execution of the Separation Statement (Form OF-109);

(c) Reviewing materials proposed for removal for all officials except Presidential appointees, located in Washington, DC, who were confirmed by the Senate.

(d) Ensuring that departing officials receive a mandatory briefing and that all departing officials will execute a Classified Information Nondisclosure Agreement (Form SF-312) certifying that they have not retained in their possession classified or administratively-controlled documents.

(2) The Department of State Records Officer *(A/RPS/IPS),* assisted by the Office of the Legal Adviser, Executive Secretariat, and the Bureau of Diplomatic Security, has oversight responsibility for the removal of documentary materials and provides overall guidance.

(3) Departing officials must ensure that all record material that they possess is incorporated in the Department's official files and that all file searches for which they have been tasked have been completed, such as those required to respond to FOIA, Congressional, or litigation-related document requests.

b. **Removal Procedures**.

(1) Classified Information. All Department of State employees are responsible for relinquishing all classified and administratively controlled documents at separation, including copies of classified documents. The following guidance applies to the declassification and access to classified documents after departure.

(a) An individual may request the declassification of specified documents, but the documents must not be removed until they have been declassified and their removal as nonrecord copies is authorized as required by these procedures.

(b) Department of State officials appointed by the President and confirmed by the Senate who wish, after their departure, to have access to classified documents they originated, reviewed or signed while serving as a Presidential appointee, may apply for such access in accordance with 22 CFR 171.25.

(2) Unclassified Papers and Materials.

(a) The departing official or a staff member must prepare an inventory of personal papers and nonrecord materials proposed for removal. The inventory need not be a listing of documents, but rather a description of categories of documents; e.g., "Resumes, Personal Correspondence, Documents Related to Financial Disclosure, and Copies of Speeches".

(b) When the inventory is completed, the departing official must request a review of the materials proposed for removal. In the Department, the Records Officer in cooperation with the Executive Secretariat or appropriate administrative office will conduct the review for Presidential appointees confirmed by the Senate. The administrative or executive office conducts the review for other Department officials and/or employees. At foreign service posts and domestic field offices, the Administrative Officer will conduct the review for all officials. Reviewing officials will consult with the Department's Records Officer as necessary.

(c) The purpose of the review is to certify that the documentary materials proposed for removal may be removed without diminishing the official records of the Department; violating national security, privacy or other restrictions on disclosure; or exceeding normal administrative economies. This generally requires a hands-on examination of the materials to verify the accuracy of the inventory.

(d) Once the reviewing official is satisfied that documentary materials proposed for removal, comply with Federal law and regulations, the reviewing official completes Form DS-1904, Authorization for the Removal of Personal Papers and Non-Record Materials, and forwards the form and the inventory to the Department of State records officer.

(3) Nonrecord materials may be removed only when authorized by the Department and only to the extent that their removal does not:

(a) Diminish the official records of the Department;

(b) Violate confidentiality required by national security, privacy or other restrictions on disclosure (e.g. commercial or financial information, personnel files or investigative records);

(c) Exceed normal administrative economies (a charge for excessive copies is within the discretion of the Department).

(4) The Department's records officer or Administrative Officer reviews the inventory, examines the materials further if necessary, and certifies the materials for removal by signing Form DS-1904, Authorization for the Removal of Personal Papers and Non-Record Materials. A copy of Form DS-1904 and the inventory are given to the departing official and a copy is retained in the reviewing office.

5 FAH-4 H-219 NON-PAPER RECORDS

(TL:RMH-3; 06-15-2000)

a. Many records of both temporary and long term value are stored in electronic media. This media can be floppy (flexible) disks, hard disks, optical disks, CD-ROM, and audio, video or magnetic tapes. These records can be duplicates of paper records or can be major information systems. Even though they may be duplicates of paper records, the electronic record in and of itself warrants special preservation. Electronic records can cover a variety of subjects from purely administrative matters to foreign policy. They can be created as word processing documents, spread sheets, or on data bases.

b. Additional guidance on electronic records that is available in OMB Circular A-130, the Federal Information Resources Management Regulation, Chapter 36 of the Code of Federal Regulations, and various regulatory bulletins from the General Services Administration and National Archives and Records Administration, can be obtained by contacting *A/RPS/IPS*. GSA's publication: "Applying Technology to Records Systems—A Media Guideline" (KML-93-1-R) also contains information on electronic records.

5 FAH-4 H-219.1 File Management

(TL:RMH-3; 06-15-2000)

a. Department offices and posts usually allow management of electronic files to be handled by system managers. Offices and posts, however, are to establish written policy regarding the disposition and review of these files to see that unique records are properly preserved.

b. Electronic files are usually accessible by date or through an index or key words for retrieval.

(1) Department offices establish procedures for the retention of on-line or off-line storage of electronic records in conjunction with *A/RPS/IPS*.

(2) Posts establish procedures for the retention of on-line or off-line storage of electronic records and coordinate with the post information management or information program officer and post systems manager (if any).

5 FAH-4 H-219.2 Security

(TL:RMH-1; 10-30-1995)

a. Special precaution is given to the security of electronic records. Because of the ability to compact large volumes of records onto small media, if compromised, more data can be exposed than in a paper file. Such laws and regulations as the Computer Fraud and Abuse Act of 1986, Computer Security Act of 1987, OMB Circular A-130, and the Federal Information Resources Management Regulations address guidelines and procedures that are used by records managers and systems administrators in protecting electronic records.

b. Additional guidance, pertinent to the Department, can be obtained from the Bureau of Diplomatic Security (DS/CIS/IST).

5 FAH-4 H-219.3 Selection and Maintenance of Electronic Records Storage Media

(TL:RMH-3; 06-15-2000)

a. Based upon guidance contained in FIRMR Bulletin B-1, administrators of electronic record systems select appropriate media and systems for storing Department records throughout their life cycle, which meet the following requirements:

(1) Permit easy retrieval in a timely fashion;

(2) Facilitate distinction between record and nonrecord material;

(3) Retain the records in a usable format until their authorized disposition date; and

(4) When appropriate meet requirements for transferring permanent records to NARA contained in 36 CFR 1228.188. Contact *A/RPS/IPS* for more information on these transfer requirements.

b. The following factors are to be considered before selecting a storage media or converting from one medium to another:

(1) The authorized life of the records, as determined during the scheduling process;

(2) The maintenance necessary to retain the records;

(3) The cost of storing and retrieving the records;

(4) The records density;

(5) The access time to retrieve records;

(6) The portability of the medium (that is, selecting a medium that will run on equipment offered by multiple manufacturers) and the ability to transfer the information from one medium to another (such as from optical disk to magnetic tape); and

(7) Whether the medium meets the current applicable Federal Information Processing Standards (FIPS). Contact *A/RPS/MMS* for information and copies of FIP standards.

c. Administrators of electronic records systems should:

(1) avoid the use of floppy disks for the exclusive long-term storage of permanent or unscheduled electronic records;

(2) see that all authorized users can identify and retrieve the information stored on diskettes, removable disks, tapes, or other media by establishing or adopting procedures for external labeling;

(3) see that information is not lost because of changing technology or deterioration by converting storage media to provide compatibility with the agency's current hardware and software. Before conversion to a different medium, administrators must determine that the authorized disposition of electronic records can be implemented after conversion; and

(4) back up electronic records on a regular basis to safeguard against loss of information due to equipment malfunction or human error. Duplicate copies of permanent or unscheduled records will be maintained in storage areas separate from the location of the records that have been copied.

5 FAH-4 H-219.4 Facsimile Transmissions

(TL:RMH-3; 06-15-2000)

a. The method of transmitting a document does not relieve sending or receiving offices of their responsibility for adequately and properly documenting official actions and activities and for ensuring the integrity of records.

b. Personnel using FAX machines to transmit memorandums, letters, or other documents that fall within the definition of a Federal record are responsible for:

(1) Obtaining appropriate clearances;

(2) Assuring that all appropriate offices receive copies of documents transmitted; and

(3) Providing copies of official written documentation, e.g. congressional correspondence, diplomatic notes, general correspondence, memoranda, and intelligence reports to *A/RPS/IPS/AAS*, for inclusion in the Department's central foreign policy file.

c. Filing record copies of documents at the time of receipt.

(1) This guidance does not apply to transitory documents. Transitory documents relate to matters of short-term interest on which no documented action is taken. They do not need to be filed.

(2) This guidance does not apply to advance copies of documents where no action is taken until receipt of the official document. Such advance copies are non-record materials and may be destroyed upon receipt of the official document.

(3) This guidance does apply to advance copies of documents if the receiving office circulates the advance copy for official purposes such as approval, comment, action, recommendation, or follow-up. In such instances, the advance copy is to be filed.

5 FAH-4 H-219.5 Oral Histories

(TL:RMH-1; 10-30-1995)

a. **Content**. Oral history materials refer to all documents, regardless of media, pertaining to interviews developed expressly for historical purposes. Such interviews are initiated with systematic questions and conducted by historians to obtain and record verbatim information from people who have participated in, or been witness to events, situations, and activities that the Department deems historically significant. Planning documents, interview scripts, and indices which may be accumulated in connection with oral histories are part of the Department's documentation.

b. **File Managemen**t. *A/RPS* is responsible for establishing standards for oral histories in conjunction with the Office of the Historian.

c. **File Arrangement and Blocking.** There is no special blocking required for these records. It is required only that they be arranged in some logical sequence.